AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method of encrypting data suitable for sending to a decrypting party, said method including the steps of:

(a) dividing said data into data segments;

(b) accepting at least a cryptographic key k shared with the decrypting party;

(c) ~~for the *i*th data segment (*i* = 1, 2 ...,) to be encrypted,~~ generating the *i*th segment key s_i for each corresponding *i*th data segment (*i* = 1, 2 ...,) to be encrypted, the *i*th segment key s_i being generable using a ~~first function~~ sequence generating function with said cryptographic key *k* and some accessory data strings as inputs;

(d) encrypting the *i*th data segment using a ~~second function~~ high-speed cipher with s_i as the encryption key to form the *i*th ciphertext segment; and

(e) outputting the *i*th ciphertext segment, and at least a part of said accessory data strings for sending data to the decrypting party, and if more data segments are to be encrypted, repeating steps (c), (d) and (e).

2. (Original) A method according to claim 1 wherein said accessory data strings include a single string v_i derived from the previous value v_{i-1} in a predetermined fashion.

3. (Currently Amended) A method according to claim 2 wherein said string vi is derived according to the relation vi = F(vi-1), i = 1, 2, ..., wherein F() is a hash function for mapping

maps vi-1 to vi and vo is an initialization value made known to the decrypting party.

4. (Previously Presented) A method according to claim 1 wherein step (e) includes outputting the size of the corresponding data segment.

5. (Currently Amended) A method according claim 1 wherein said ~~first function~~ sequence generating function includes a ~~cryptographic~~ pseudo random sequence generator.

6. (Currently Amended) A method according to claim 5 wherein said pseudo random sequence generator includes a keyed hash function $h(k, v_{i1}, v_{i2}, \ldots, v_{il})$, wherein k is said cryptographic key, $(v_{i1}, v_{i2}, \ldots, v_{il})$ is said accessory data strings and l is a positive integer.

7. (Currently Amended) A method according to claim 6 wherein the keyed hash function $h()$ is MD5 or SHA.

8. (Previously Presented) A method according to claim 1 wherein said accessory data strings are derived from various sources.

9. (Original) A method according to claim 8 wherein said sources include current time and date, or previous accessory data strings, or some initialization values, or at least a part of the data segments or previous ciphertext segments, or at least a part of previous segment keys.

10. (Original) A method according to claim 1 wherein said accessory data strings include two

parts, one part being derived by the decrypting party in a predetermined fashion prior to decrypting said *i*th ciphertext segment and the other part not being derived by, and therefore being sent to, the decrypting party prior to decrypting said *i*th ciphertext segment.

11. (Currently Amended) A method according to claim 1 wherein said ~~second function~~ high-speed cipher includes an encryption function of a symmetric key cipher.

12. (Currently Amended) A method according to claim 1 wherein said ~~second function~~ high-speed cipher includes an encryption function of a block cipher operating in a well known mode, such as Electronic Code Book mode.

13. (Currently Amended) A method according to claim 1 wherein said ~~second function~~ high-speed cipher includes an encryption function resulting from combined use of more than one symmetric key cipher.

14. (Currently Amended) A method of decrypting data encrypted by an encrypting party, said method including the steps of:

(a) accepting at least a cryptographic key k being shared with the encrypting party;

(b) for the *i*th ciphertext segment ($i = 1, 2, ...,$) to be decrypted, generating the *i*th segment key s_i using a ~~first function~~ sequence generating function with said cryptographic key k and some accessory data strings as inputs;

(c) decrypting the *i*th ciphertext segment using a ~~second function~~ high-speed cipher with s_i as the decryption key;

(d) outputting the decrypted *i*th ciphertext segment, and if more ciphertext segments are to be decrypted, repeating steps (b), (c) and (d).

15. (Original) A method according to claim 14 wherein said accessory data strings include a single string vi derived from the previous value vi-1 in a predetermined fashion.

16. (Currently Amended) A method according to claim 15 wherein said string vi is derived according to the relation vi = F(vi-1), i = 1, 2, ..., wherein F() is a hash function for mapping ~~maps~~ vi-1 to vi and vo is an initialization value made known to the encrypting party.

17. (Currently Amended) A method according to claim 14 wherein said ~~first function~~ sequence generating function includes a ~~cryptographic~~ pseudo random sequence generator.

18. (Currently Amended) A method according to claim 17 wherein said pseudo random sequence generator includes a keyed hash function $h(k, v_{i1}, v_{i2}, ..., v_{il})$, wherein k is said cryptographic key, $(v_{i1}, v_{i2}, ..., v_{il})$ is said accessory data strings and l is a positive integer.

19. (Currently Amended) A method according to claim 18 wherein the keyed hash function *h*() is MD5 or SHA.

20. (Previously Presented) A method according to claim 14 wherein said accessory data strings include two parts, one part being derived by the decrypting party in a predetermined fashion from available sources prior to decrypting said *i*th ciphertext segment and the other part

not being derived by, and therefore being received by, the decrypting party prior to decrypting said *i*th ciphertext segment.

21. (Currently Amended) A method according to claim 14 wherein said ~~second function~~ high-speed cipher includes a decryption function of a symmetric key cipher.

22. (Currently Amended) A method according to claim 14 wherein said ~~second function~~ high-speed cipher includes a decryption function of a block cipher operating in a well known mode, such as Electronic Code Book mode.

23. (Currently Amended) A method according to claim 14 wherein said ~~second function~~ high speed function includes a decryption function resulting from a combined use of more than one symmetric key cipher.

24. (Currently Amended) Apparatus for encrypting data suitable for sending to a decrypting party, said apparatus including:

(a) means for dividing said data into data segments;

(b) means for accepting at least a cryptographic key k shared with the decrypting party;

(c) means for generating for the *i*th data segment (i = 1, 2, ...,) to be encrypted, the *i*th segment key s_i using a ~~first function~~ sequence generating function with said cryptographic key *k* and some accessory data strings as inputs;

(d) means for encrypting the *i*th data segment using a ~~second function~~ high-speed cipher with S_i as the encryption key to form the ith ciphertext segment; and

(e) means for outputting the ith ciphertext segment, and at least a part of said accessory data strings for sending data to the decrypting party.

25. (Original) Apparatus according to claim 24 wherein said accessory data strings include a single string V_i derived from the previous value V_{i-1} in a predetermined fashion.

26. (Currently Amended) Apparatus according to claim 25 wherein said string V_i is derived according to the relation $V_i = F(V_{i-1})$, $i = 1, 2, ...,$ wherein $F()$ is a hash function for mapping ~~maps~~ V_{i-1} to V_i and V_o is an initialization value made known to the decrypting party.

27. (Previously Presented) Apparatus according to claim 24 wherein said means for outputting is adapted for outputting the size of the corresponding data segment.

28. (Currently Amended) Apparatus according to claim 24 wherein said ~~first function~~ sequence generating function includes a ~~cryptographic~~ pseudo random sequence generator.

29. (Currently Amended) Apparatus according to claim 28 wherein said pseudo random sequence generator includes a keyed hash function $h(k, V_{i1}, V_{i2}, ..., V_{il})$, wherein k is said cryptographic key, $(V_{i1}, V_{i2}, ..., V_{il})$ is said accessory data strings and l is a positive integer.

30. (Currently Amended) Apparatus according to claim 29 wherein the keyed hash function $h()$ is MD5 or SHA.

31. (Previously Presented) Apparatus according to claim 24 wherein said accessory data strings are derived from various sources.

32. (Original) Apparatus according to claim 31 wherein said sources include current time and date, or previous accessory data strings, or some initialization values, or at least a part of the data segments or previous ciphertext segments, or a part of previous segment keys.

33. (Original) Apparatus according to claim 24 wherein said accessory data strings include two parts, one part being derived by the decrypting party in a predetermined fashion prior to decrypting said *i*th ciphertext segment and the other part not being derived by, and therefore being sent to, the decrypting party prior to decrypting said *i*th ciphertext segment.

34. (Currently Amended) Apparatus according to claim 24 wherein said ~~second function~~ high-speed cipher includes an encryption function of a symmetric key cipher.

35. (Currently Amended) Apparatus according to claim 24 wherein said ~~second function~~ high-speed cipher includes an encryption function of a block cipher operating in a well known mode, such as Electronic Code Book mode.

36. (Currently Amended) Apparatus according to claim 24 wherein said ~~second function~~ high-speed cipher includes an encryption function resulting from combined use of more than one symmetric key cipher.

37. (Currently Amended) Apparatus for decrypting data encrypted by an encrypting party, said apparatus including:

(a) means for accepting at least a cryptographic key k being shared with the encrypting party;

(b) means for generating as inputs for the *i*th ciphertext segment (*i* = 1. 2, ...,) to be decrypted, the *i*th segment key s_i using a ~~first function~~ sequence generating function with said cryptographic key *k* and some accessory data strings;

(c) means for decrypting the *i*th ciphertext segment using a ~~second function~~ high-speed cipher with s_i as the decryption key; and

means for outputting the decrypted *i*th ciphertext segment.

38. (Original) Apparatus according to claim 37 wherein said accessory data strings include a single string v_i derived from the previous value v_{i-1} in a predetermined fashion.

39. (Currently Amended) Apparatus according to claim 38 wherein said string v_i is derived according to the relation $v_i = F(v_{i-1})$, *i* = 1, 2, ..., wherein *F*() is a hash function for mapping ~~maps~~ v_{i-1} to v_i and v_o is an initialization value made known to the encrypting party.

40. (Currently Amended) Apparatus according to claim 37 wherein said ~~first function~~ sequence generating function includes a ~~cryptographic~~ pseudo random sequence generator.

41. (Currently Amended) Apparatus according to claim 40 wherein said pseudo random sequence generator includes a keyed hash function $h(k, v_{i1}, v_{i2}, ..., v_{il})$, wherein *k* is said

cryptographic key, (V_{i1}, V_{i2}, ..., V_{il}) is said accessory data strings and l is a positive integer.

42. (Currently Amended) Apparatus according to claim 41 wherein the keyed hash function *h()* is MD5 or SHA.

43. (Previously Presented) Apparatus according to claim 37 wherein said accessory data strings include two parts, one part being derived by the decrypting party in a predetermined fashion from available sources prior to decrypting said *i*th ciphertext segment and the other part not being derived by, and therefore being received by, the decrypting party prior to decrypting said *i*th ciphertext segment.

44. (Currently Amended) Apparatus according to claim 37 wherein said ~~second function~~ high-speed cipher includes a decryption function of a symmetric key cipher.

45. (Currently Amended) Apparatus according to claim 37 wherein said ~~second function~~ high-speed cipher includes a decryption function of a block cipher operating in a well known mode, such as Electronic Code Book mode.

46. (Currently Amended) Apparatus according to claim 37 wherein said ~~second function~~ high-speed cipher includes a decryption function resulting from a combined use of more than one symmetric key cipher.